IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
BEAUMONT DIVISION

PETER HARRIS AND LONI HARRIS, *Plaintiffs,* VS. UPWINTRADE.COM, A BUSINESS ASSOCIATION; DAVID SHAMLIAN, AN INDIVIDUAL; JOHN DOES 1 – 20, *Defendants.*	§ § § § § § § § § § §	CIVIL ACTION NO. 1:24-CV-00313 JUDGE MICHAEL J. TRUNCALE

ORDER GRANTING PLAINTIFFS' MOTION FOR EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER AUTHORIZING EXPEDITED DISCOVERY

Plaintiffs have filed an Emergency Motion for Emergency *Ex Parte* Temporary Restraining Order and Order Authorizing Expedited Discovery (the "Motion") [Dkt. 2], in which they seek an order requiring the freezing of the accounts associated with twenty-nine deposit addresses at four cryptocurrency exchanges and authorization to issue subpoenas to various third parties who they claim are likely to be in possession of information about the Defendants. The Court has reviewed Plaintiffs' Motion and supporting evidentiary materials. For the reasons set out herein, Plaintiffs' Motion is hereby **GRANTED**.

I. Background

Plaintiffs' relevant allegations are as follows. In February 2024, Plaintiff Loni Harris saw a Facebook post that appeared to be authored by a friend of hers from high school. ECF. 1, Verified Complaint (henceforth "Complaint"), ¶ 14. This post

alluded to the friend's recent financial successes, which had purportedly been achieved under the guidance of a person named "David." *Id*. Interested, Ms. Harris sent a message to the account that appeared to be operated by her old friend. *Id*. This person recommended that Ms. Harris contact one David Shamlian.[1] *Id*.

Ms. Harris reached out to Shamlian, who offered her his tutelage in cryptocurrency-related investment and trading. *Id*. at ¶ 15. Soon, Ms. Harris's husband, Peter Harris, connected with Shamlian as well. *Id*. Shamlian told the Harrises that in order to take advantage of his proprietary trading strategies, they would need to make an account on a cryptocurrency-trading platform called Upwintrade. *Id*. The Harrises soon did so. *Id*.

Over the course of the next several months, Shamlian 'trained' the Harrises in the process of using the Upwintrade platform. *Id*. at ¶ 16. First, he instructed them to make their own accounts at well-established cryptocurrency exchanges, which they did. *Id*. They then deposited their own U.S. Dollars into those accounts, which they used to buy Bitcoin. Then, following Shamlian's instructions, they would transfer their Bitcoin to "deposit addresses" provided to them on the Upwintrade platform. *Id*. They repeated this process in a series of transactions from February to May 2024, ultimately transferring Bitcoin with transfer-date value of more than $650,000.00 to the addresses provided to them by Upwintrade. *Id*.

[1] The Harrises allege that they later confirmed that this account was not created by Loni Harris's friend, but was instead a fraudulent account impersonating that friend without his knowledge. *Id*.

Each time the Harrises made a 'deposit' to their Upwintrade account, the account balance presented in their user portal increased as expected. *Id*. In other words, the platform appeared to be working, from their perspective. And in fact, just as Shamlian had promised, their balance began to grow rapidly as they profited from his strategies and Upwintrade's purportedly advanced technology. *Id*. at ¶ 17.

Then, in May 2024, the Harrises decided to withdraw some of their assets from Upwintrade. *Id*. But they were told they could not make a withdrawal until they paid hundreds of thousands of dollars in "taxes" to "release" their account. *Id*. The Harrises began to suspect that they had been the victims of a scam and retained counsel. *Id*. Despite their repeated entreaties, Upwintrade never returned their assets. *Id*.

The Harrises now allege that Upwintrade's explanations as to why they could not withdraw their funds were lies. *Id*. at ¶ 18. They say the real reason Upwintrade would not return their assets is that Upwintrade is not a trading platform at all. *Id*. Instead, they claim that they have been the victims of a "pig-butchering scam" operated by the Defendants. *Id*. at ¶ 4. According to the Harrises, this is a type of investment scam in which the perpetrators deceive victims into depositing their assets on a fake-but-realistic-looking "trading" or "investment" platform where no trading or investment ever occurs. *Id*. Instead, the Harrises allege, the assets are simply stolen. *Id*.

Evidentiary materials submitted by the Harrises suggest that these kinds of investment scams are now amongst the most prevalent forms of cybercrime

worldwide. ECF No. 2, Ex. 1-C, Affidavit of Evan Cole (henceforth "Cole Affidavit") (providing excerpts from FBI Internet Crime Report). These materials also show that the Harrises' experience is very similar to the experiences of other pig-butchering victims described in journalistic outlets and law-enforcement reports. *Id.*, Exs. 1-A (article describing typical pig-butchering scam), 1-B (Secret Service Bulletin describing pig-butchering scams), 1-C (excerpts from FBI Internet Crime Report).

After retaining counsel, the Harrises engaged an investigator to perform a "blockchain tracing" report. This "tracing" refers to the process of following digital assets from location to location on the blockchain via publicly available data. Cole Affidavit at ¶ 7. The Harrises' investigator was able to trace their stolen assets to addresses associated with four distinct cryptocurrency exchanges: (1) Binance, (2) Revolut, (3) Remitano, and (4) ByBit. *Id.* at ¶¶ 8 - 12. In the instant Motion, the Harrises ask the Court to order that these exchanges temporarily freeze the accounts associated with the blockchain addresses they have identified as receiving the assets stolen from them, so that they might preserve some assets for recovery.

In addition, by investigating Upwintrade.com and David Shamlian's personal website, the Harrises have identified several additional third parties they claim are likely to be in possession of information about the Defendants. These third parties include, for example, the companies these websites used for web hosting and live-chat functionality. The Harrises' Motion seeks to issue subpoenas to these third parties, in addition to the four cryptocurrency exchanges mentioned above, with the

aim of revealing the Defendants' true identities and unearthing contact information that they might subsequently use to serve or otherwise communicate with them.

II. Analysis

The Harrises have met the requirements for issuance of a temporary restraining order and expedited discovery for the following reasons.

A. Temporary Restraining Order

The standard for issuance of an *ex parte* temporary restraining order has both procedural and substantive elements. Procedurally, the Court has the authority to issue an *ex parte* restraining order where (i) "specific facts in an affidavit or a verified complaint clearly show that immediate and irreparable injury, loss, or damage will result to the movant before the adverse party can be heard in opposition," and (ii) "the movant's attorney certifies in writing any efforts made to give notice and why it should not be required." FED. R. CIV. P. 65(b)(1)(A)-(B).

Both requirements are met here. The Harrises' Verified Complaint and the Cole Affidavit show the likelihood of immediate and irreparable injury or loss. These materials suggest that the Harrises were in fact the victims of a prevalent form of cybercrime—the "pig-butchering scam"—which features well-established and recognizable patterns of deception. *See* Complaint, ¶¶ 14 – 19; Cole Affidavit, ¶¶ 3 – 5 (concluding that the Harrises were the victim of a pig-butchering scam and providing news reports and law-enforcement bulletins for comparison). The Cole Affidavit further details how the assets allegedly stolen from the Harrises could be further transferred to unretrievable locations at any time, with the click of a button.

Cole Affidavit, ¶ 13 (explaining that "crypto assets can be moved in seconds from address to address," and that the Harrises will be unlikely to recover their assets if they are further dissipated). Several federal courts have found that this exigency justified issuance of *ex parte* restraining orders in similar crypto-fraud cases, and this Court finds their reasoning persuasive here.[2]

In addition, the Harrises attorney has certified why notice should not be required. As the Harrises point out in their Motion, the Court has the authority to enter an *ex parte* order not only where notice to the adverse party is impracticable, but where "notice to the defendant would render fruitless [the] prosecution of the action." *Matter of Vuitton et Fils S.A.*, 606 F.2d 1, 5 (2d Cir. 1979); *see also, e.g.*, *First Tech. Safety Sys., Inc. v. Depinet*, 11 F.3d 641, 650 (6th Cir. 1993) (noting that *ex parte* order is justified where "the adverse party has a history of disposing of evidence or violating court orders or [] persons similar to the adverse party have such a history"). Under this logic, courts have found that notice of an asset-freeze motion is not required if the parties to be enjoined "are likely to dissipate assets and destroy business documents," such that the very act of providing notice would

[2] *See, e.g.*, *Ohlin v. Defendant 1*, No. 3:23-C-8856-TKW-HTC, 2023 WL 3676797, at *3 (N.D. Fla. May 26, 2023) ("Considering the speed with which cryptocurrency transactions are made as well as the anonymous nature of those transactions, it is imperative to freeze the Destination Addresses to maintain the status quo to avoid dissipation of the money illegally taken from Plaintiffs."); *Jacobo v. Doe*, No. 1:22-CV-00672DADBAKBAM, 2022 WL 2052637, at *3 (E.D. Cal. June 7, 2022) ("Because it would be a simple matter for [defendant] to transfer [the] cryptocurrency to unidentified recipients outside the traditional banking system and effectively place the assets at issue in this matter beyond the reach of the court, the court finds that plaintiff is likely to suffer immediate and irreparable harm in the absence of injunctive relief.") (cleaned up); *Astrove v. Doe,* No. 1:22-CV-80614-RAR, 2022 WL 2805315, at *3 (S.D. Fla. Apr. 22, 2022) (same).

"cause immediate and irreparable injury or damages to the Court's ability to award effective final relief." *Fed. Trade Comm'n v. Dluca*, No. 18-60379-CIV, 2018 WL 1830800, at *2 (S.D. Fla. Feb. 28, 2018), *report and recommendation adopted*, No. 0:18-CV-60379-KMM, 2018 WL 1811904 (S.D. Fla. Mar. 12, 2018). Several courts have found that this same reasoning justified issuance of *ex parte* freezing orders in crypto-fraud cases analogous to this one.[3]

Here, the thrust of the Harrises' allegations is that the Defendants are professional cybercriminals who have every motivation to place their ill-gotten gains beyond the reach of this Court or any other authority. While at this stage these are simply allegations, the Harrises have provided sufficient evidence to suggest that the Defendants will in fact further dissipate assets if they were given notice of this motion. This is sufficient to justify issuance of an *ex parte* order under these unique circumstances.

Having found that the procedural requirements for issuance of an *ex parte* restraining order are met, the Court now turns to the substantive standard. To obtain a temporary restraining order, a movant must show (1) a substantial

[3] *See, e.g.*, *Gaponyuk v. Alferov*, No. 223CV01317KJMJDP, 2023 WL 4670043, at *2 (E.D. Cal. July 20, 2023) (issuing *ex parte* asset-freeze TRO in similar crypto-fraud case, and writing that "federal district courts have granted *ex parte* relief in situations like this one, noting the risks that cryptocurrencies may rapidly become lost and untraceable"); *Ohlin*, 2023 WL 3676797, at *2 (notice not required where plaintiff offered declarations showing that the defendants were crypto-criminals, which gave the court "every reason to believe the Defendants would further hide those [stolen] assets if they were given notice"); *Jacobo*, 2022 WL 2052637, at *3 (notice not required because plaintiff made credible allegations that defendants were crypto-criminals, which "pose[d] a heightened risk of asset dissipation").

likelihood of success on the merits, (2) a substantial threat of irreparable harm if the injunction does not issue, (3) that the threatened injury outweighs any harm that will result if the injunction is granted, and (4) that the grant of an injunction is in the public interest. *Moore v. Brown*, 868 F.3d 398, 402-03 (5th Cir. 2017).

The Harrises have met each of these requirements. On the merits, the Harrises make claims against the Defendants for violation of the Racketeering Influenced and Corrupt Organizations Act ("RICO"), fraud, and conversion. Complaint, ¶¶ 21 – 32. They have alleged and provided evidence that the Defendants deceived them and misappropriated their assets in what appears to have been an intentional pig-butchering scam. Complaint, ¶¶ 1 – 4, 14 – 19; Cole Affidavit, ¶¶ 3 – 5. The Court finds, at this stage, that the similarities between Plaintiffs' allegations and the widely known characteristics of this distinctive kind of scam suggest that they will indeed be able to prevail on these claims against the Defendants once a full evidentiary record is developed. In addition, the Court notes that asset freeze the Harrises seek in this instance is permissible in light of their request for a constructive trust over specific, traceable stolen assets, as several courts have held in analogous cryptocurrency-fraud cases. *See, e.g.*, *Yogaratnam v. Dubois*, No. CV 24-393, 2024 WL 758387, at *3 (E.D. La. Feb. 23, 2024) (issuing asset-freeze TRO in crypto-fraud case, noting that "numerous district courts … have issued a TRO in this exact circumstance to freeze a cryptocurrency asset," and collecting cases); *Jacobo*, 2022 WL 2052637, at *3 (issuing asset-freezing TRO

where plaintiff sought constructive trust over allegedly stolen assets); *Gaponyuk*, 2023 WL 4670043, at *2 (same).

The Harrises have also shown that irreparable harm will ensue absent the restraining order they seek, for the same reasons explained above. In light of the speed with which cryptocurrency transactions are made, as well as the potential that the Defendants may further move the assets they are alleged to have stolen, the Court finds that the Harrises' request to freeze the exchange accounts to which those assets were transferred is justified, as have other courts considering similar circumstances. *See Jacobo*, 2022 WL 2052637, at *3.

Next, the Court finds that the threatened injury to the Harrises outweighs any harm the Defendants may suffer by virtue of a freeze of their accounts. Maintaining the assets at the destination accounts is perhaps the Harrises' only realistic chance at a future recovery in this case. In contrast, as other courts have reasoned, the Court finds that the Defendants will suffer at worst a temporary inability to move assets if the injunction is later dissolved. *See Jacobo*, 2022 WL 2052637, at *6 (same, finding "[a] delay in defendant's ability to transfer the [allegedly stolen] assets only minimally prejudices defendant, whereas withholding injunctive relief would severely prejudice plaintiff by providing defendant time to transfer the allegedly purloined assets into other accounts beyond the reach of this court").

Finally, the Court finds that issuing the injunction is in the public interest. The Harrises have adduced evidence showing that they are but two of many victims

of what appears to be an epidemic of similar scams. Cole Affidavit, ¶¶ 3 – 5 (describing pig-butchering scams as "epidemic" and providing law-enforcement and academic materials suggesting that Americans have lost billions to such scams). A freezing order will serve the public interest here both by dissuading would-be fraudsters from preying on American citizens, and providing assurance to the public that courts will take action to promote … recovery of stolen assets when they can be readily located and traced to specific locations." *Jacobo*, 2022 WL 2052637, at *6; *see also, e.g.*, *Gaponyuk*, 2023 WL 4670043, at *3 (finding that asset freeze would "serve the public's interest in stopping, investigating, and remedying frauds").

B. Expedited Discovery

Typically, parties may not seek "discovery from any source before the conference required by Rule 26(f)." FED R. CIV. P. 26(d)(1). But expedited discovery before a Rule 26(f) conference is permitted where "authorized … by court order." *Id.* Courts in this circuit apply a "good cause" standard to determine whether such an order should issue. *St. Louis Grp., Inc. v. Metals & Additives Corp.*, 275 F.R.D. 236, 239 (S.D. Tex. 2011) (applying good cause standard). Good cause may be found where "the need for expedited discovery in consideration of the administration of justice, outweighs the prejudice to the responding party." *Id.* at 239.

Courts have authorized expedited discovery from cryptocurrency exchanges in cryptocurrency-related fraud cases like this one. *See, e.g.*, *Strivelli v. Doe*, No. 22-cv-22060 2022 WL 1082638, at *2 (D.N.J. Apr. 11, 2022) (authorizing expedited discovery from cryptocurrency exchanges in crypto case and noting "the Court's

review of cryptocurrency theft cases reveals that courts often grant motions for expedited discovery to ascertain the identity of John Doe defendants"); *Licht v. Ling*, No. 3:23-cv-1018, 2023 WL 4504585 (N.D. Tex. June 20, 2023), at *4 (issuing broad authorization for expedited discovery in analogous crypto-fraud case and requiring that "any party served with a request for production shall produce all requested items within 72 hours of the request"). Indeed, in similar cases, courts have held that any privacy interests that alleged cybercriminals have concerning the discovery of information about their identities and activities is outweighed by the need to adjudicate victims' claims against them. *Gaponyuk*, 2023 WL 4670043, at *4 (finding alleged cybercriminals' privacy interests were "outweighed by the need to adjudicate the [victim's] claims," and holding that "privacy concerns shall not be a just cause for [a] subpoenaed non-party to withhold [] requested documents and information").

Here, the Harrises' proposed discovery arises from their pre-suit blockchain tracing and investigation of the Defendants' web properties. These investigations revealed a series of third parties likely to be in possession of information about the Defendants. Each of those third parties and their connection to this case is set out below.

Subpoena Target	***Alleged Connection to Case***	***Evidence***
Microsoft Corporation	Microsoft owns Skype, the messaging app the Harrises allege they used to communicate with Shamlian.	Exhibit 1-H

Meta Platforms, Inc.	Meta owns Facebook, where the alleged deception at issue in this case began and where the Harrises communicated with the defendants.	Exhibit 1-I
SRS AB	The Harrises have submitted evidence showing that SRS AB is the domain registrar for Upwintrade.com.	Exhibit 1-J
Mastercard Inc.	The Harrises have submitted evidence showing that, at some point, a Mastercard payments processing tool was installed on the site.	Exhibit 1-K
Visa Inc.	The Harrises have submitted evidence showing that, at some point, a Mastercard payments processing tool was installed on the site.	Exhibit 1-K
Data Room, Inc.	The Harrises have submitted evidence showing that Data Room provided the U.S.-based servers from which the Defendants operated upwintrade.com.	Exhibit 1-J
LLC Technology Distribution Ltda	The Harrises have submitted evidence showing that entity owns and operates JivoChat, a live-chat plugin that the Defendants used to communicate with victims on Upwintrade.com.	Exhibit 1-L
Wild West Domains, LLC	The Harrises have submitted evidence showing that this entity is the domain registrar for davidshamlian.com, the personal website of David Shamlian.	Exhibit 1-M
OrangeHost LLC	The Harrises have submitted evidence showing that this entity provides web-hosting services for davidshamlian.com.	Exhibit 1-M
Elementor Ltd.	The Harrises have submitted evidence showing that the Defendants used the Elementor site-building tool to build the website at davidshamlian.com.	Exhibit 1-N

Binance, Ltd.	The Harrises allege that a significant portion of the cryptocurrency the Defendants stole from them was ultimately deposited in accounts at the Binance cryptocurrency exchange.	Exhibit 1-F
Revolut Technologies, Inc.	The Harrises allege that a significant portion of the cryptocurrency the Defendants stole from them was ultimately deposited in accounts at Revolut, which is a "neo-bank" that offers both crypto- and fiat-denominated accounts.	Exhibit 1-F
Babylon Solutions Limited	This entity owns and operates the peer-to-peer cryptocurrency exchange Remitano. The Harrises allege that a significant portion of the Bitcoin that the Defendants stole from them was ultimately transferred to Remitano accounts.	Exhibit 1-F
Bybit Fintech Limited	The Harrises allege that a significant portion of the Bitcoin that the Defendants stole from them was ultimately deposited in accounts at the Bybit cryptocurrency exchange.	Exhibit 1-F

The Harrises request the Court's authorization to issue subpoenas to each of the above-listed entities seeking the following information. For all targets, the Harrises seek to discover all biographical and contact information associated with the Defendants' accounts. They also seek to discover IP-address and location logs showing the devices and locations from which the Defendants accessed these accounts.

The Harrises also seek to discover any payments information in the subpoena targets' possession, including the Defendants' transaction histories and information

about the credit or debit cards the Defendants used to pay for the subpoena targets' services. As to the Defendants' payment methods, the Harrises seek only information sufficient to identify the Defendants' payments provider and the Defendants' account with that provider.

Finally, as to the firms to which the Harrises' stolen assets were transferred—*i.e.*, Binance, Revolut, Bybit, and Remitano—the Harrises seek to discover the current account balances associated with the Defendants' accounts, their transaction histories, and identification of any other accounts on the respective platforms associated with the accountholders by re-use of biographical or contact information.

Courts have authorized similar discovery where the plaintiff adduced evidence that the persons about whom the information was sought were cybercriminals and the plaintiff also sought a temporary restraining order freezing the assets held in those accounts. *Strivelli*, 2022 WL 1082638, at *2 (granting broad expedited discovery in analogous crypto-fraud case); *see also Licht*, 2023 WL 4504585, at *4 (same). The Court finds these courts' reasoning persuasive, and therefore authorizes the scope of discovery requested by the Harrises here.

III. Relief Granted

A. Restraining Order

The Plaintiffs have submitted evidence tracing the assets they allege were stolen from them to 29 deposit addresses at the cryptocurrency exchanges Binance,

Revolut, Remitano, and ByBit (the "Receiving Addresses"). The Receiving Addresses are:

Exchange	**Address**
Binance	13mLDAfVfyzD8Vf6x9YZ5pALc3g8TXqPix
Binance	1MUxDUmHAVskKATJDCWgk8SJ9ZBHreZAbh
Binance	1DMhMwn4apg49oVjRpbaZqJDDLJaN6iqox
Binance	13WWx7qQ1QBoY2E3sjaRrzvWzg2JJkDAgg
Binance	1PvjGd7aCpvRzZtz4kL9YgdvnYPdpm16oj
Revolut	bc1q7gku9m33re89mes97dwq4lawwxg3hj6g28umcy
Remitano	38ZWvd5Be2PqMu5xcvy9PY3T4frKvniNyf
Remitano	38Ep5mFzh6oNbuFXSL1Hvk3g1TwXUMX8xv
Remitano	3M5RWiGdcEDRseLUqaG15HgPLL7bf3644A
Remitano	3A34Ggh1EUNXe4K8ayTLNLdKYAUDTnEU63
Remitano	3MoVdQzjhYJrz9umg4v1oBRRz5pe9kZVcu
Remitano	3A3NqjhLiexUzcfgGuVo19uzux8rnbqSVE
Remitano	3CaPngqFGiu8kSLEcp9uM5JvK97RdAGHBU
Remitano	3KE6diBJr2yCcd9HEUxH5KNd86s2tzPW2N

Remitano	3B9GDHG6WgrWeavz247zAvbd5WrC8rYF7y
Remitano	3KKGPBqG2GW5PNVmktjoJwsSoGmfrvVTBB
Remitano	3G1gfTQn81jgaPUCWCoSr8j17AtiWn17uy
Remitano	3DGPG9Lh6iLSkxYf9UZxzxjcUKo36xUva9
Remitano	3D8JCs231iJxK8Jx86pJ4TAWrAAtbRxRPW
Remitano	33heGnSTbA6U7WrfMBYoWYgCRBek2MrKTA
Remitano	3AymDrgNq3WQZaNLh4vxLe8bxVzGaHqQhz
Remitano	31jJbyCxErbbfkuGP1dtz2Pz9jt9SWNv83
Remitano	35wtpq7h7AjMP2xaS9yNa8T9cgJfUUm5RW
Remitano	3BjbZnAwmmxvQFnibcyGRd8SAwM6xTLYpA
Remitano	3CZ6NHrctR8ceWwyYyJQXP96PMAqEs5J4a
Remitano	3KSpJdiRmej8XkqCYswa58pff127b7nQxc
Remitano	39TPPnjRGB8ANVbs1K7RFoBBDNtvXWtECj
ByBit	1HyTkypyP8yoRGSRrvr74SyEhhX1bkLMiQ
ByBit	14rxMsRQV5fkTDb3ShorD91xQvdwp34hjb

For the reasons set out in the Motion, the Court finds that the accounts associated with these deposit addresses should be frozen. Accordingly, the Court

hereby **ORDERS** that Defendants and their agents, servants, employees, attorneys, partners, successors, assigns, and all other persons or entities through which they act or who act in active concert or participation with any of them, who receive actual notice of this Order by personal service or otherwise, whether acting directly or through any trust, corporation, subsidiary, division or other device, or any of them, are hereby restrained from withdrawing, transferring, or encumbering any assets currently held by, for, or on behalf of the persons controlling the accounts associated with the above-listed Receiving Addresses, or any business entity through which they act or which acts in active concert or participation with them; including those assets currently held at or for the Receiving Addresses.

In accordance with Fed. R. Civ. P. 65(b)(2), this Order will expire fourteen (14) days from its entry unless it is extended for good cause shown. No bond shall be required to be posted by Plaintiff.

B. Expedited Discovery

The Court finds that Plaintiffs' request to issue expedited discovery should be granted for the reasons set out above. Plaintiffs are authorized to serve subpoenas on the third parties identified above. In light of the time-sensitivity of Plaintiffs' subpoenas to the cryptocurrency exchanges to which their assets were ultimately transferred, Plaintiffs are authorized to serve this Order on these exchanges via email directed to the following addresses:

Recipient	Service Address
Binance, Ltd.	legal@binance.com compliance@binance.com
Revolut Technologies, Inc.	legal@revolut.com compliance@revolut.com
Babylon Solutions Limited	legal@remitano.com compliance@remitano.com
ByBit Fintech Limited	legal@bybit.com compliance@bybit.com

All subpoenaed parties shall produce the materials sought in the subpoena to Plaintiffs' counsel within seven (7) days of their receipt of Plaintiffs' subpoena and this Order.

The Court finds that any privacy interest the Defendants have in the documents requested by Plaintiffs is outweighed by the need to investigate and prosecute the theft and conversion alleged in the complaint. Such privacy concerns shall not be good cause for the subpoenaed party to withhold the requested material.

SIGNED this 8th day of August, 2024.

Michael J. Truncale
Michael J. Truncale
United States District Judge